(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 September 2003 (18.09.2003)

PCT

(10) International Publication Number
WO 03/077498 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/CA03/00315

(22) International Filing Date: 7 March 2003 (07.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/362,865 8 March 2002 (08.03.2002) US

(71) Applicant *(for all designated States except US)*: **CERTICOM CORP.** [CA/CA]; 4th Floor, 5520 Explorer Drive, Mississauga, Ontario L4W 5L1 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **STRUIK, Marinus** [NL/CA]; 728 Manning Ave., Toronto, Ontario M6G 2W4 (CA). **VANSTONE, Scott, Alexander** [CA/CA]; 10140 Pineview Trail, P.O. Box 490, Campbellville, Ontario L0P 1B0 (CA).

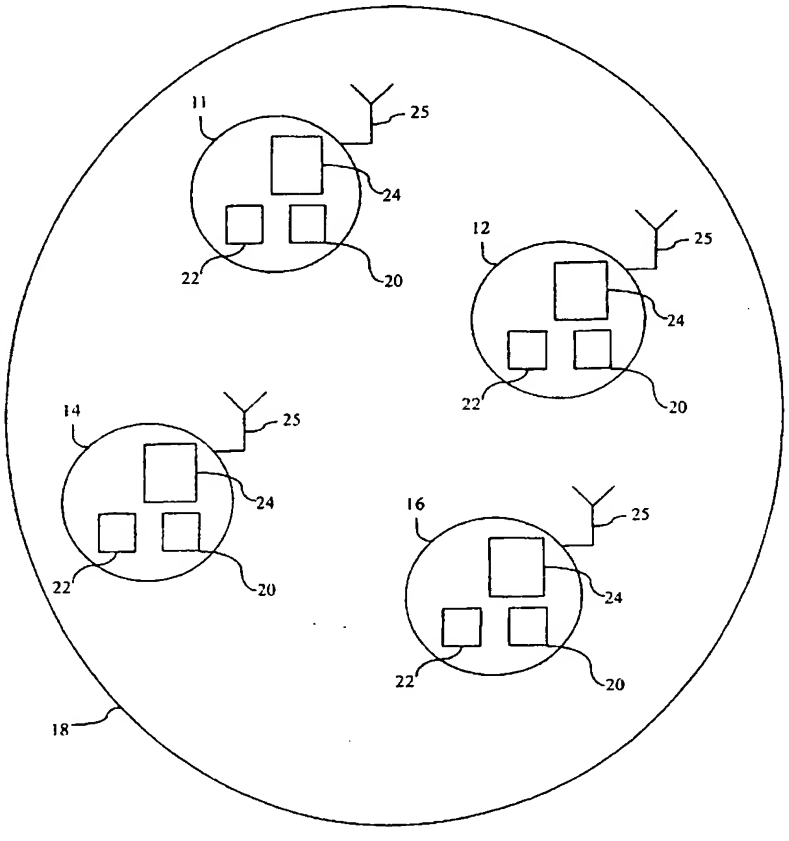
(74) Agents: **ORANGE, John, R., S.** et al.; McCarthy Tetrault LLP, Suite 4700, P.O. Box 48, 66 Wellington St. W., Toronto, Ontario M5K 1E6 (CA).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: LOCAL AREA NETWORK



(57) Abstract: A method and system for distributed security for a plurality of devices in a communication network, each of the devices being responsible for generating, distributing and controlling its own keys for access to the communication network and using the keys to establish a trusted network, each device's membership to the communication network being checked periodically by other devices by using a challenge response protocol to establish which devices are allowed access to the communication network and the trusted network.

WO 03/077498 A1

Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

LOCAL AREA NETWORK

BACKGROUND OF THE INVENTION

[0001] This application claims priority in United States Provisional Application Serial No. 60/362,865, entitled "Local Area Network", filed on March 8, 2002 and United States Provisional Application Serial No. 60/363,309, entitled "Local Area Network", filed on March 11, 2002.

FIELD OF THE INVENTION

[0002] This invention relates to communication networks, more particularly it relates to security within these networks.

DESCRIPTION OF THE PRIOR ART

[0003] One of the most significant recent developments in wireless technologies is the emergence of wireless personal area networking. Wireless personal area networks WPANs™ use radio frequencies to transmit both voice and data, and are specified by standards such as IEEE standard 802.15 or 802.3 from the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA), among other specifications. The 802.15 specification is ideal for linking notebook computers, mobile phones, personal digital assistants (PDAs), digital cameras, and other handheld devices to do business at home, on the road, or in the office.

[0004] These wireless networks are formed by a number of devices joining and leaving the network in an ad hoc manner, hence such networks are known as ad hoc networks or piconets. Thus, the set of devices connected to the ad hoc network any given time may fluctuate, and so the topology of the network is dynamic. It is desirable to control access to the network and to provide a mechanism for establishing and maintaining security. Traditionally, security is established using a central device or a piconet controller (PNC) which controls access and distributes keys within the network. A drawback of this scheme is that each member of the network is required to trust the PNC.

[0005] Admission to the piconet is based on the outcome of the following protocols between the prospective joining device and the PNC of the piconet. The joining device and the PNC engage in a mutual entity authentication protocol based on public key or symmetric key techniques. The true device identity of both the joining device and the PNC is determined using this protocol. A link key can also be derived based on the authentic keys of both parties. Another protocol involves using authorization techniques between both devices, based on access control lists (ACLs). The Access Control Lists may be dynamically updated, similar to PDA functionality, where a determination is made whether an entity is added or removed from the ACL at entry. This determination may be made by an operator, such as a human operator. For devices that lack a user interface, this update mechanism may be invoked by an open enrollment period followed by a lock-up step, for example, which may be confirmed by a button push or be a simple re-set of the whole list. This may be performed by actuating a re-set or re-initialize button on the device.

[0006] Thus devices in the piconet fully depend on information provided by the PNC regarding which devices have been admitted to the piconet, since admission is based on communication between the PNC and a joining device only. If however an improper list of devices, DeviceList, in the piconet has been distributed by the PNC, either by error or maliciously, the security of the network is jeopardised. Each device has a short hand address, such as a local 8-bit ID, and a long hand address, such as a global 48-bit device ID. For example, in a piconet in which since all devices share a common broadcast key, the list of admitted devices to the piconet is L:= (local 8-bit device ID, global 48-bit device ID), then the failure to obtain the complete and authentic list of admitted devices has the following consequences:

[0007] *`Fly on the wall'* scenario:

[0008] If a device obtains an incomplete list: $L' \subset (L' \neq L)$ of admitted devices, all devices in the complementary set $L \setminus L'$ are `invisible' to the device. Hence, the device might mistakenly think it is sharing secured information only with devices from the list L', whereas actually it is unknowingly sharing with other devices of the set L as well. This obviously violates sound security practice.

[0009] *'Switchboard'* scenario ' :

[0010] If the binding between the local device ID and the global device ID is incorrectly received, for example if 2 entries are interchanged, a device might direct information to the improper device and so compromise the intended security. This property also holds in other settings where a key-generating party does not share complete and authentic information on the composition of the key-sharing group itself with the other members of this group. Therefore, these scenarios present a security model in which there is complete trust or a security model in which a device trusts no other device, however a hybrid model of these two models is possible.

[0011] Accordingly it is an object of the present invention to mitigate or obviate at least one of above-mentioned disadvantages.

SUMMARY OF THE INVENTION

[0012] In one of its aspects the invention provides a method of establishing and maintaining distributed security between a plurality of devices in an ad hoc network, the method having the steps of; associating each device with a unique device address;

assigning to one of the devices a control function to control access to the network by other devices;

each of the devices generating a public key for distribution to other devices;

each of the devices authenticating itself periodically with the other devices in order to determine status of the other devices;

arranging the devices into a plurality of trust groups, each group having a group key for distribution within the trust group;

associating a trust level to each of the devices;

each of the devices using the public key and the group key to perform key agreement in order to establish a secure communication channel with the other devices in the group;

whereby each of the devices is responsible for its own security by generating, distributing its own keys to the other devices.

[0013] In another aspect, the invention provides a method of establishing and maintaining distributed security between one correspondent and another correspondent, the correspondents being members of different ad hoc networks and forming a group of communicating correspondents, the method having the steps of;

associating the one correspondent and the other correspondent with unique device addresses;

controlling access to the different ad hoc networks;

each ad hoc network having a gateway and transferring traffic between the correspondents via the gateways;

the one correspondent generating a public key for distribution to the other correspondent;

the one correspondent authenticating itself periodically with the other correspondent in order to determine status of the other correspondent;

determining a group key for distribution to the correspondents in accordance to the step of controlling access;

associating a trust level to each correspondent; each of the correspondents using the public key and the group key for performing key agreement in order to establish secure communication within the group;

whereby the one correspondent is responsible for its own security by generating, distributing its own keys to the other correspondent.

[0014] In yet another aspect, the invention provides a distributed security system for a plurality of devices in a network, each of the devices being responsible for generating, distributing and controlling its own keys for access to the network and using the keys to establish a trusted network, each device's membership to the network being checked periodically by other devices by using a challenge response protocol to establish which devices are allowed access to the network and the trusted network.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] These and other features of the preferred embodiments of the invention will become more apparent in the following detailed description in which reference is made to the appended drawings wherein

[0016] Figure 1 is a communication network;

[0017] Figure 2 is a group structure for a security model having different trust levels;

[0018] Figure 3 is a group structure for a security model having different trust levels;

[0019] Figure 4 is a group structure for a security model having different trust levels;

[0020] Figure 5 is a group structure for a security model having different trust levels;

[0021] Figure 6 shows communication between piconets;

[0022] Figure 7 shows a flowchart outlining steps for establishing secure communication between devices in different piconets; and

[0023] Figure 8 shows secure communication between piconets;

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0024] Reference is first made to Figure 1, which shows an overview of a distributed security system 10 having a plurality of communication devices 11, 12, 14, 16 in a communication network 18, in a preferred embodiment. The communication network 18 may be a wireless personal area network (WPAN™) such as a piconet, in which the devices 11, 12, 14, 16 connect to each other in an ad hoc fashion. The devices 11,12, 14, 16 may be portable and mobile computing devices such as PCs, Personal Digital Assistants (PDAs), peripherals, cell phones, pagers, consumer electronics, and other handheld devices. It will be understood that such devices 11, 12, 14, 16 include addressing information to facilitate communication within the network 18. The addressing information includes a local device ID, having 8 bits for example, and a device ID, such as, an IEEE MAC Address including 48 bits. Therefore, upon a device 11, 12, 14, 16 joining the network it is assigned an unused local ID. Generally, one device 11 will act as a master or a piconet network controller (PNC), and the other devices 12, 14, 16 act as slaves for the duration of the piconet 18 connection. The PNC 11 sets a clock , a hopping pattern determined by device ID, and assigns time for connections between all devices 11, 12, 14 16. Thus, each piconet 18 includes a unique hopping pattern/ID, and the PNC 11 gives slaves 12, 14 16 the clock and a local device ID, which is optionally used in conjunction with the EEE MAC Address, to form the piconet 18.

[0025] The PNC 11 activates an access controller 20 using ID's of the devices and optionally an access control list such that devices 12, 14, 16 that have been positively

authenticated and have been authorized are admitted to the piconet 18. The PNC 11 also includes a traffic controller 22 to regulate data flow within the network 18. This may be done by allocating time slots to each device 11,12,14,16 for message distribution. Each of the devices 11, 12, 14, 16 includes a security manager function 24. The security manager function 24 generates keys for communicating with other devices 11,12,14,16 within the network 18, and distributes these keys to selected device members 11,12,14,16 of the network 18. Each device 11, 12, 14 or16 includes a transceiver 25 for establishing a communication channel with other devices 11,12,14,16. When distributing a key, the security manager function 24 also indicates to the other devices 11,12,14,16 in the network 18 the other devices 11,12,14,16 to which the key is being distributed. Thus, there is no reliance on other devices 11, 12, 14, 16 for trust functionality, as each device 11, 12, 14 or 16 need only trust itself, to form a distributed security regime.

[0026] Thus, the security manager function 24 can establish a trust set, or TrustList, which indicates which of the devices 11,12,14,16 in the network the security manager 24 of that particular device 11,12,14 or 16 is prepared to trust. The security manager function 24 may also attribute different levels of trust to each of the established trust sets. In this way the equivalent of a centralised network 18 can be established where a device 11,12,14 or 16 trusts every other device 11,12,14 or 16; or an entirely decentralised network 18 is provided where a device 11,12,14 or 16 trusts no other device 11,12,14 or 16 but itself.

[0027] Similarly the security manager 24 receiving a key from another device 11, 12, 14, 16 can determine its source and allocate to that key a level of trust that determines the functions for which the key will be used. Thus the security manager 24 may determine that the key is from a trusted party 11, 12, 14 or 16 and the key may be used to both decrypt messages received from that trusted party 11, 12, 14 or 16 and encrypt messages sent to that trusted party 11, 12, 14 or 16. Alternatively, the security manager function 24 may determine that the key originates at a party 11, 12, 14 or 16 not trusted by itself and only permit the key to be used for decryption. However, the device 11, 12, 14 or 16 may choose to ignore data, rather than going through the effort of having to decrypt the data first. This option may be useful for dealing with unsolicited communication or 'junkmail'.

[0028] The security manager 24 also includes methods of determining which of the devices 11, 12, 14 or 16 are presently active in the network 18. These methods include the functions of each device 11, 12, 14 or 16 re-authenticating itself with each of its key sharing parties 11, 12, 14 or 16 at predetermined time. One such method includes the steps of periodically performing a 'heartbeat operation' in the form of a challenge response protocol to determine which devices are presently included in the network 18, and adjusting the groups and trust levels accordingly. Thus, each device 11, 12, 14 or 16 may dynamically update its own TrustList to reflect changes in the trust relationships. For devices 11,12,14 or 16 that lack a user interface, this update mechanism may be invoked by an open enrollment period followed by a lock-up step, possibly confirmed by a button push, or it may be a simple re-set of the whole list, for example by pushing a re-set or re-initialize button on the device 11,12,14 or 16.. Moreover, some of the changes might be invoked by a third entity that performs remote or delegated trust management for that device.

[0029] Referring now to Figure 2, in order to describe the distributed security model, as an example, assume the PNC 11 permits access to devices A, B,C,D, E, F, G, H, then the DeviceSet :={A,B,C,D,E,F,G,H}. However if the device A only trusts devices A, B, C then TrustSet(A):= {A, B, C} that is Group 1. Also, device A may participate in other groups having a different trust set, such as Group 2, having only device D. Thus the security manger function 24 of device A senses Group 1 and Group 2 with different constituent members and different levels of trust. For example, in Group 1, if device C is the key source, and since device C is part of the TrustSet(A), this key by device C is distributed which is used for both encryption/decryption permitted as C, and device A only accepts keys transferred to itself by devices DEV $\in$TrustSet(A), for encryption and decryption purposes. In Group 2, as device D is not part of TrustSet(A), then A accepts a key from device D, and any other devices E, F,G and H, which are not part of TrustSet(A), for decryption purposes only. Accordingly if device A desires to communicate to Group2 members, the device A generates a new group key to form a new group, Group 3, and device A distributes this new group key to the members of Group2', that is device D. Therefore, the groups then under the control of the security manager of

device A will then be Group 1, Group 2, as mentioned above, and Group 3, as shown Figure 3.

[0030] The flexibility of the security managers 24 of devices A, B, C, D, E, F, G, H permits different network structures to be mimicked. For example, using the notation above, if DeviceSet :={A,B,C,D,E,F,G,H}, and TrustSet(A):=Universe, then device A ca be considered an altruistic device which provides a structure equivalent to a centralized model. Conversely, if TrustSet(D):={D}, then device D is an egocentric device, and is a structure equivalent a completely decentralized model. Then, looking at Figure 4, device A participates in Groups 1, 2 and 3, all groups having with differing trust relationships. For example, in Group 1 having devices A, B and C, if the key source is device C, then this group key is used for encryption and decryption, as device A trusts all devices B,C,D,E,F,G and H, which of course includes the key source C. However, in Group 2 having devices A, D, and G, with the key source being device G, once again device A uses this group key is used for encryption and decryption, while device D uses it for decryption only as it does not trust any other device A,B,C,E,F,G or H. In Group 3 having devices D and E, with the key source being device E, device D uses the group key for decryption only as it does not trust device E. As device A is not included in Group 3, it does not receive the key.

[0031] In Figure 5, where one of the device F is hidden from the other members in the network 18, then Group 2 does not include the full list of member devices, A,D,G and H. Therefore, device D can not communicate with device F as the heartbeat operation will indicate that device D is not alive. Since the 8-bit address or the 48-bit address of device is unavailable, there is no communication between D and device F. Therefore, device D uses the group keys for decryption only.

[0032] Thus, these different group structures as shown in Figures 2, 3, 4 and 5 may be established within the same network 18 by using a decentralised or distributed security management scheme having the ability to set different levels of trust per device. This may be used in a number of ways, such as admission of devices A, B, C, D, E, F, G and H, such as PDAs to a piconet 18 based on different subscription models. For example, one subscription model may include charging a fee for airtime/bandwidth fee, while another model may be based on charging for content. In this example, the models may be

implemented in a building, such as an airport or fitness club, the network 18 includes a fixed PNC 11 on a ceiling and the PNC 11 multicasting to subscribing devices only, or the models may be implemented between individual devices. Thus, by separating the role of the security manager 24 from that of the PNC 11, charging models that differentiate between airtime/bandwidth cost and content/subscription cost are possible, as these charging models might be operated by different entities A,B,C,D,E,F,G or H, or another intermediate entity.

[0033] It will be seen therefore that a versatile network 18 is provided, and moreover the removal of a device A,B,C,D,E,F,G or H from the network 18 does not require re-establishment of all keys in the network 18 as the individual devices A,B,C,D,E,F,G or H control the distribution of the keys. Figure 6 shows communication between a device A in piconet 1 with another device B in piconet 2, where Z_1 and Z_2 are members of piconet 1 and piconet 2, respectively. Z_1 and Z_2 include transceivers 25 for establishing a communication channel or relay channel 26 between piconet 1 and piconet 2. Thus, Z_1 listens in on all traffic and sends all traffic destined for device B to Z_2 via the relay channel 26. Upon receipt of the traffic relayed by Z_1 , Z_2 further broadcasts this traffic to B. Z_1 and Z_2 include WPAN functionality and may act as data relay agents only, and thus may not process data. Piconet 1 and piconet 2 include respective PNC_1 and PNC_2 and thus devices A and B only need PNC_1 and PNC_2 , respectively, for allocation of time slots, and the function of protection of content is performed by the security manager 24 of each device A, B.

[0034] In order to facilitate communication between devices A and B, in different piconets 1 and 2, device A is associated with a router 28 which stores information related to other devices in its piconet 1, and routing information having instructions on how to route traffic from device A to other devices, such as device B. Correspondingly, device B is also associated with a router 30 having similar functionalities. Thus, any device A or B is associated with a router and these routers 28, 30 query each other periodically in order to update router information, due to the dynamic nature of the ad hoc networks 18.

[0035] Referring to Figure 7 and Figure 8, in order to establish a secure communication between device A and B, device A performs the steps of acquiring device B's full static address or device ID and a public key or symmetric key in order to perform

key agreement, in step 110. In the next step 112, the key agreement yields an authentication key for subsequent communication. Once device A receives a response, in predetermined time, that proves possession of the group public key, in step 114, then device A generates a new set of group keys and transports these keys to device B, in step 116. Device B can then acknowledge receipt of group keys in step 118. Thus, devices A and B require each other's authentic public key and each other's full device ID for authentication and establishment of a secure channel 26, as different piconets may use different short hand address addresses for each device A or B. Therefore, device A and device B form a trusted group and a secure channel is set up if device B trusts any of the intermediate routers, otherwise device B creates its own keys in order to set up a secure channel 26

[0036] Although the invention has been described with reference to certain specific embodiments, various modifications thereof will be apparent to those skilled in the art without departing from the spirit and scope of the invention as outlined in the claims appended hereto.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of establishing and maintaining distributed security between a plurality of devices in an ad hoc network, the method having the steps of;

associating each device with a unique device address;

assigning to one of said devices a control function to control access by other devices to said network;

each of said devices generating a public key for distribution to other devices;

each of said devices authenticating itself periodically with said other devices in order to determine status of said other devices;

arranging said devices into a plurality of trust groups, each group having a group key for distribution within said trust group;

associating a trust level to each of said devices;

each of said devices using said public key and said group key to perform key agreement in order to establish a secure communication channel with said other devices in said group;

whereby each of said devices is responsible for its own security by generating, distributing its own keys to said other devices.

2. The method of claim 1 wherein said device determines a source of said group key.

3. The method of claim 2 wherein when said source is a device in said trust group then said group key is used for encryption and decryption of data transmitted between said devices.

4. The method of claim 2 wherein when said source is a device excluded trust group then said group key is used decryption of data transmitted to said device.

5. The method of claim 1 wherein step of determining status of said other devices includes a further step of determining which of said devices are active and capable of participating in said network.

6. The method of claim 1 wherein step of determining status of said other devices includes a further step of using a challenge response protocol using said group key to establish whether said other devices are allowed access to said network in accordance with said control function.

7. The method of claim 1 wherein said unique device address includes a device ID or a local ID.

8. The method of claim 7 wherein said device ID is an IEEE MAC address and said local ID is an n-bit address unique to said group.

9. A method of establishing and maintaining distributed security between one correspondent and another correspondent, said correspondents being members of different ad hoc networks and forming a group of communicating correspondents, the method having the steps of;

associating said one correspondent and said other correspondent with a unique device address;

controlling access to said different ad hoc networks;

each ad hoc network having a gateway and transferring traffic between said correspondents via said gateways;

said one correspondent generating a public key for distribution to said other correspondent;

said one correspondent authenticating itself periodically with said other correspondent in order to determine status of said other correspondent;

determining a group key for distribution to said correspondents in accordance to said step of controlling access;

associating a trust level to each of said correspondents;

each of said correspondents using said public key and said group key for performing key agreement in order to establish secure communication within said group;

whereby each of said correspondents is responsible for its own security by generating, distributing its own keys to said other devices.

10. The method of claim 9 wherein said step of transferring traffic includes a further step of associating each of said correspondents with a router for storing routing information having instructions for routing traffic from said one correspondent to said other correspondent.

11. The method of claim 10 wherein said routers query each other periodically in order to update and maintain said routing information.

12. The method of claim 11 wherein said step of determining said status of said other correspondent includes a further step of using a challenge response protocol to establish whether said other correspondent is allowed access to said different ad hoc network having said one correspondent, in accordance with said control function.

13. A distributed security system for a plurality of devices in a communication network, each of said devices being responsible for generating, distributing and controlling its own keys for access to said communication network and using said keys to establish a trusted network, each device's membership to said communication network being checked periodically by other devices by using a challenge response protocol to establish which devices are allowed access to said communication network and said trusted network.

14. The system of claim 13 wherein each device includes a security manager having the functions of generating said keys and distributing said keys to selected devices in said trusted network.

15. The system of claim 14 wherein said trusted network is associated with a level of trust.

16. The system of claim 14 wherein said security manager determines a source of said keys such that said keys from a device within said trusted network may be used for encryption and decryption of data, and said keys from a device excluded from said trusted network may be used decryption of said data.

17. The system of claim 16 wherein said security manager foregoes decrypting said data when said keys are from a device excluded from said trusted network.

18. The system of claim 15 wherein an outcome of said periodic checking is recorded by said security manager in order to maintain and update a membership list, and adjust said level of trust accordingly.

19. The system of claim 17 wherein different trusted networks may be established within said network based on differing levels of trust.

20. The system of claim 13 wherein said communication network includes a plurality of ad hoc networks and said distributed security system is established between devices in different ad hoc networks.

21. The system of claim 19 wherein each ad hoc network includes a controller to controlling access to each of said ad hoc networks, each ad hoc network having a gateway for transferring traffic therebetween, and device having a router for storing routing information having instructions for routing traffic from said one device to another device via said gateways and other routers.

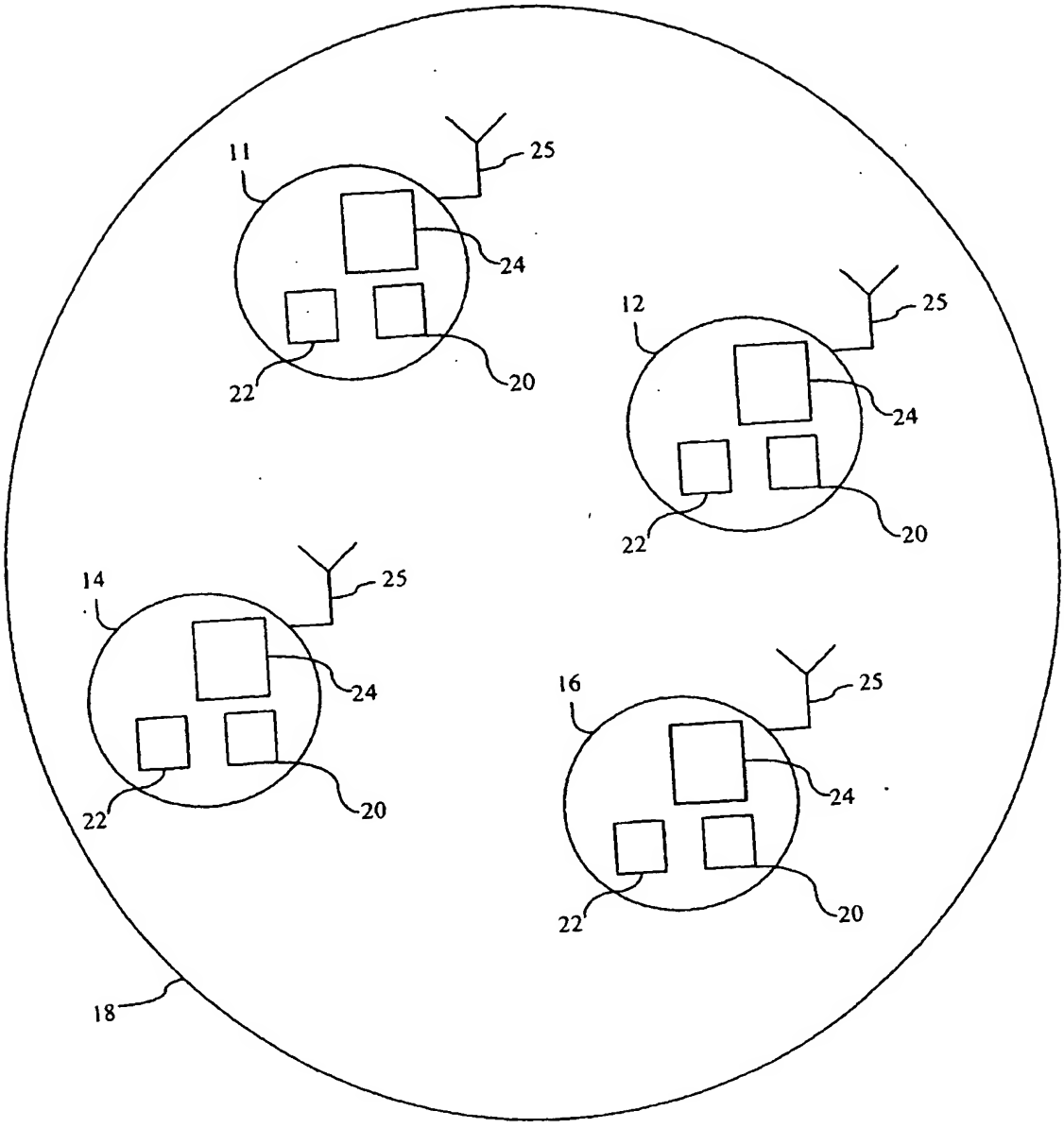


Figure 1

	A B C D E F G H		
Group l'	x x x	Key source: C	encryption/decryption permitted
Group2'	x x	Key Source: D	decryption only

Figure 2

	A B C D E F G H		
Group l'	x x x	Key source: C	encryption/decryption
Group2'	x x	Key Source: D	decryption
Group3'	x x	Key source: A	encryption/decryption

Figure 3

	A B C D E F G H		A	D
Group 1'	x x x	Key source: C	encryption/decryption	
Group2'	x x x	Key Source: G	encryption/decryption	decryption
Group3'	x x	Key Source: E		decryption

Figure 4

	A B C D E F G H		A	D
Group l	x x x	Key source: C	encryption/decryption	
Group2	x x $ x	Key Source: G	encryption/decryption	decryption
Group3'	x x	Key Source: E		decryption

$: hidden node (`fly on the wall')

Figure 5

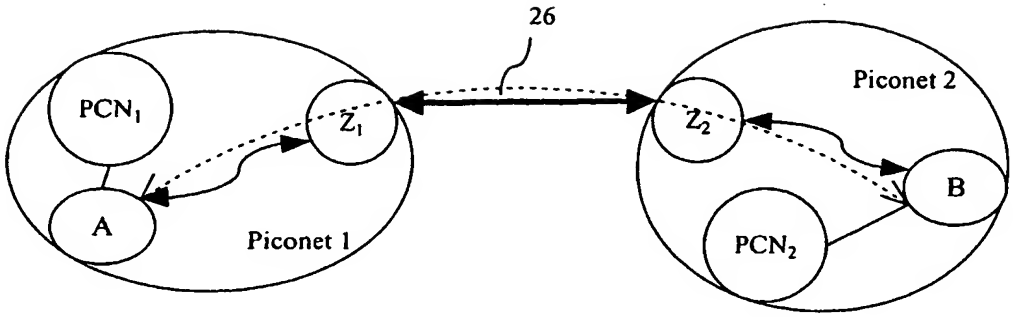


Figure 6

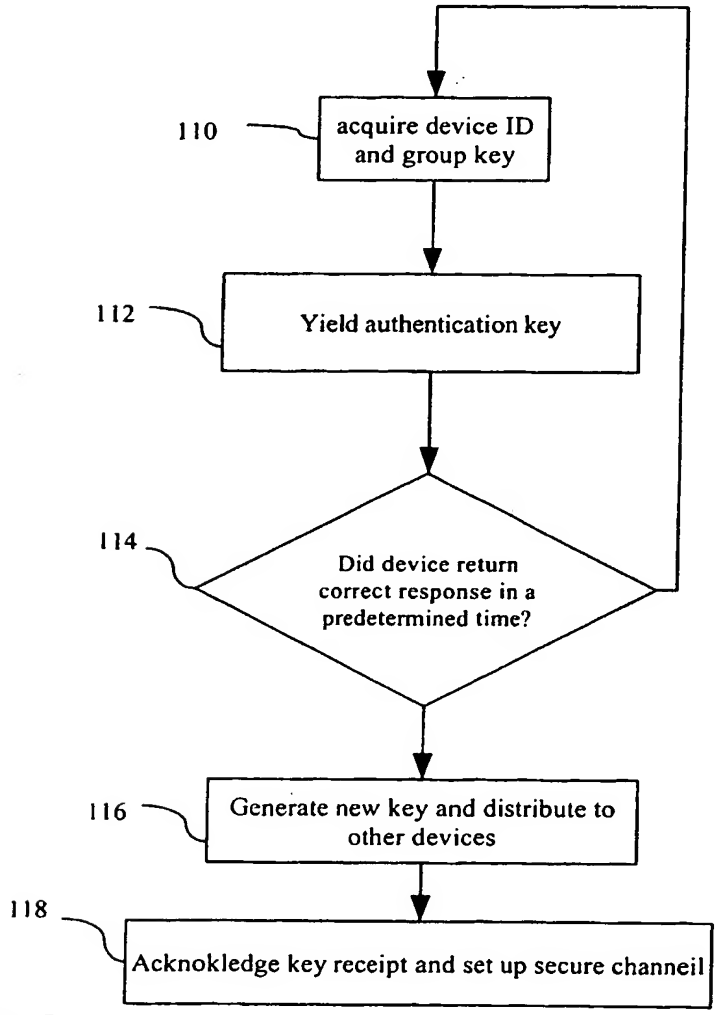


Figure 7

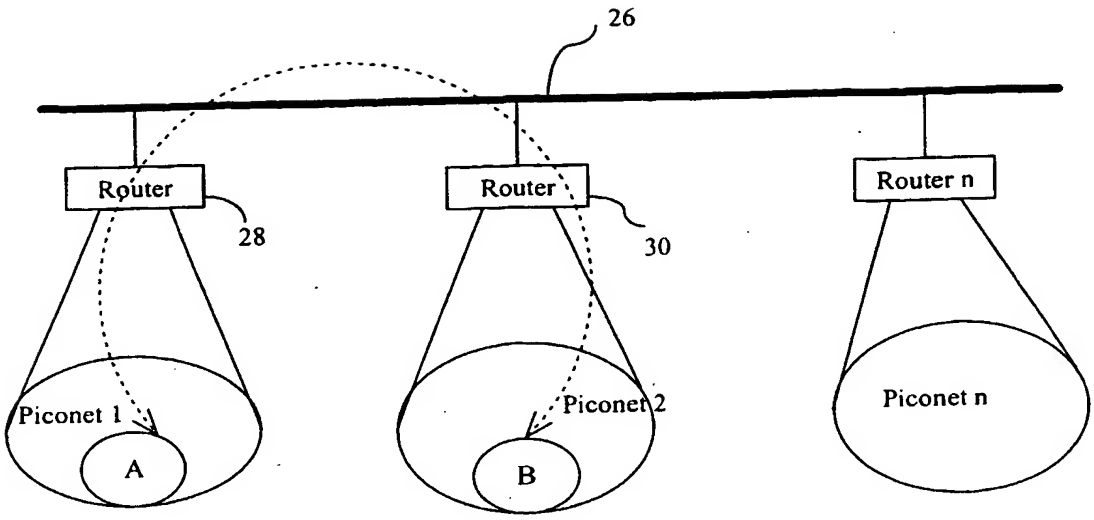

26
Router
28
Router
30
Router n
Piconet 1
A
Piconet 2
B
Piconet n

Figure 8

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA 03/00315

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	VENKATRAMAN L ET AL: "A novel authentication scheme for ad hoc networks" DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING AND COMPUTER SCIENCE, vol. 3, 23 September 2000 (2000-09-23), pages 1268-1273, XP010532729	1-3,5-7, 9-15,20, 21
A	page 1269, right-hand column, line 28 -page 1271, left-hand column, line 13 page 1272, left-hand column, line 15 -page 1273, left-hand column, line 11	4,8, 16-19

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 July 2003	16/07/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lázaro, M.L.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA 03/00315

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	JACOBS S ET AL: "MANET Authentication Architecture" INTERNET DRAFTS, March 1999 (1999-03), XP002206450 Retrieved from the Internet: <URL:http://www.watersprings.org/pub/id/draft-jacobs-imep-auth-arch-00.txt> 'retrieved on 2002-07-17!	13,14, 20,21
A	page 2, line 19-32 page 6, line 5-28 page 7, line 13 -page 8, line 15 page 13, line 19 -page 14, line 8 page 15, line 1-25 ---	1-12, 15-19
X	EP 1 102 430 A (ERICSSON TELEFON AB L M) 23 May 2001 (2001-05-23)	1-3,5,6, 13-15, 20,21
A	abstract paragraphs '0004!,'0013!,'0014!,'0019!-'0022! ---	4,7-12, 16-19
A	HAAS Z J ET AL: "The Zone Routing Protocol (ZRP) for Ad Hoc Networks" INTERNET DRAFTS, November 1997 (1997-11), XP002153515 Retrieved from the Internet: <URL:http://www.ics.uci.edu/ãtm/adhoc/paper-collection/haas-draft-ietf-manet-zone-zrp> sections 2.0,2.1,2.3 ---	10,11
A	US 5 602 916 A (GRUBE GARY W ET AL) 11 February 1997 (1997-02-11) claims 1-11 -----	1-21

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No
PCT/CA 03/00315

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1102430 A	23-05-2001	EP 1102430 A1	23-05-2001
		AU 1183701 A	08-05-2001
		CN 1415148 T	30-04-2003
		EP 1226680 A2	31-07-2002
		JP 2003513513 T	08-04-2003
		WO 0131836 A2	03-05-2001
US 5602916 A	11-02-1997	NONE	